アイゼンシュタイン数について

熊谷　隆行
学習院大学　理学部　数学科

平成 21 年 2 月 2 日

1　目的

ここでは，アイゼンシュタイン数についていろいろ調べる．
アイゼンシュタイン数の定義は次の通りである．
$a^2+ab+b^2=c^2$　を満たす正の整数 a,b,c をアイゼンシュタイン数という．
また，$(a,b,c)=1$ のとき，a,b,c を原始アイゼンシュタイン数と言う．

2　方法

2.1　方針

$a^2+ab+b^2=c^2$ を満たす (a,b,c) を考える．

2.1.1　プログラムの実行

```
ab(A,B,C,X):-X is A*A+A*B+B*B,
X0 is sqrt(X),
C is floor(X0),
C*C=:=X.

for(I =<J,I) :- I =<J.
for(I =<J,K) :- I =<J ,
I1 is I+1,for(I1 =<J,K).

nm(N,M):-
for(N=<M,A),
for(A=<M,B),
ab(A,B,C,X),
gcd3(D=[A,B,C]),
D==1,
% write(d=D),
write([A,B,C]),
```

```
put(9),write(A),put(9),write(B),put(9),write(C),nl,
fail.
nm(N,M).

gcd(D=(D,0)):-!.
gcd(D=(A,B)):-
R is A mod B,
gcd(D=(B,R)).

gcd3(D=[A,B,C]):- !,
gcd(D1=(A,B)),
gcd(D=(D1,C)).
```

2.1.2 プログラムの結果

表 1:

[a,b,c]	a	b	c	c(n+1)-c(n)	mod 6
[3, 5, 7]	3	5	7	6	0
[7, 8, 13]	7	8	13	6	0
[5, 16, 19]	5	16	19	12	0
[11, 24, 31]	11	24	31	6	0
[7, 33, 37]	7	33	37	6	0
[13, 35, 43]	13	35	43	6	0
[16, 39, 49]	16	39	49	12	0
[9, 56, 61]	9	56	61	6	0
[32, 45, 67]	32	45	67	6	0
[17, 63, 73]	17	63	73	6	0
[40, 51, 79]	40	51	79	12	0
[11, 85, 91]	11	85	91	0	0
[19, 80, 91]	19	80	91	6	0
[55, 57, 97]	55	57	97	6	0
[40, 77, 103]	40	77	103	6	0
[24, 95, 109]	24	95	109	18	0
[13, 120, 127]	13	120	127	6	0
[23, 120, 133]	23	120	133	0	0
[65, 88, 133]	65	88	133	6	0
[69, 91, 139]	69	91	139	12	0
[56, 115, 151]	56	115	151	6	0
[25, 143, 157]	25	143	157	6	0
[75, 112, 163]	75	112	163	6	0
[15, 161, 169]	15	161	169	12	0
[104, 105, 181]	104	105	181	12	0
[32, 175, 193]	32	175	193	6	0
[56, 165, 199]	56	165	199	12	0

表 2:

[29, 195, 211]	29	195	211	6	0
[17, 208, 217]	17	208	217	0	0
[87, 160, 217]	87	160	217	6	0
[85, 168, 223]	85	168	223	6	0
[119, 145, 229]	119	145	229	12	0
[31, 224, 241]	31	224	241	6	0
[72, 203, 247]	72	203	247	0	0
[93, 187, 247]	93	187	247	12	0
[64, 221, 259]	64	221	259	0	0
[144, 155, 259]	144	155	259	12	0
[19, 261, 271]	19	261	271	6	0
[95, 217, 277]	95	217	277	6	0
[133, 192, 283]	133	192	283	18	0
[40, 279, 301]	40	279	301	0	0
[136, 209, 301]	136	209	301	6	0
[35, 288, 307]	35	288	307	6	0
[105, 247, 313]	105	247	313	18	0
[21, 320, 331]	21	320	331	6	0
[105, 272, 337]	105	272	337	6	0
[37, 323, 343]	37	323	343	6	0
[111, 280, 349]	111	280	349	12	0
[185, 231, 361]	185	231	361	6	0
[88, 315, 367]	88	315	367	6	0
[152, 273, 373]	152	273	373	6	0
[176, 259, 379]	176	259	379	18	0
[23, 385, 397]	23	385	397	6	0
[80, 357, 403]	80	357	403	0	0
[115, 333, 403]	115	333	403	6	0
[161, 304, 409]	161	304	409	12	0
[41, 399, 421]	41	399	421	6	0
[123, 352, 427]	123	352	427	0	0
[240, 253, 427]	240	253	427	6	0
[48, 407, 433]	48	407	433	6	0
[205, 299, 439]	205	299	439	18	0
[240, 287, 457]	240	287	457	6	0
[43, 440, 463]	43	440	463	6	0
[25, 456, 469]	25	456	469	0	0
[129, 391, 469]	129	391	469	12	0
[175, 369, 481]	175	369	481	0	0
[215, 336, 481]	215	336	481	6	0
[88, 437, 487]	88	437	487	12	0
[275, 301, 499]	2754	301	499	12	0

表 3:

[104, 451, 511]	104	451	511	0	0
[264, 325, 511]	264	325	511	12	0
[208, 387, 523]	208	387	523	18	0
[184, 425, 541]	184	425	541	12	0
[135, 473, 553]	135	473	553	6	0
[141, 475, 559]	141	475	559	0	0
[189, 440, 559]	189	440	559	12	0
[235, 416, 571]	235	416	571	6	0
[297, 368, 577]	297	368	577	12	0
[329, 351, 589]	329	351	589	24	0
[280, 423, 613]	280	423	613	6	0
[245, 459, 619]	245	459	619	42	0
[319, 441, 661]	319	441	661	12	0
[377, 400, 673]	377	400	673	30	0
[312, 493, 703]	312	493	703	36	0
[371, 480, 739]	371	480	739	24	0
[403, 477, 763]	403	477	763	54	0
[448, 495, 817]	448	495	817	-817	5

3 考察

この結果を見ると, c に関して，特徴が表れている．c に出てきた数を考えると，$c\,(n+1)-c\,(n)$ は，$6K$（$K \geq 0$）の形で表すことができる.（(mod 6 が 0 ）の形.）よって，c に関しては，$6K+1$ の形で表すことが出来る.

3.1 方針

それでは，もう少し c について考察してみよう．プログラムの結果に出てきた c を素因数分解してみる.

3.1.1 プログラムの実行

```
factor(P/2):- Q is P//2,P =:= 2*Q,!.
factor(P/I):- P1 is floor(sqrt(P)),
        for(1 =< P1,J),
              J1 is 2*J+1,
Q is P//J1,
          P =:= J1*Q,I= J1,!.
factor(P/P) :- !.
```

```
factorize(P,[P]):- factor(P/P1),P1==P,!.
factorize(P,List):- factor(P/I),
P1 is P//I,
List=[I|List1],
factorize(P1,List1),!.

kakeru([A],A):-!.
kakeru([A,B],A*B):-!.
kakeru([A|List],X):-length(List,S),S>1,
kakeru(List,Y),X= A*Y.
```

3.1.2 プログラムの結果

表 4:

[a,b,c]	a	b	c	c の素因数分解
[3, 5, 7]	3	5	7	7
[7, 8, 13]	7	8	13	13
[5, 16, 19]	5	16	19	19
[11, 24, 31]	11	24	31	31
[7, 33, 37]	7	33	37	37
[13, 35, 43]	13	35	43	43
[16, 39, 49]	16	39	49	7*7
[9, 56, 61]	9	56	61	61
[32, 45, 67]	32	45	67	67
[17, 63, 73]	17	63	73	73
[40, 51, 79]	40	51	79	79
[11, 85, 91]	11	85	91	7*13
[19, 80, 91]	19	80	91	7*13
[55, 57, 97]	55	57	97	97
[40, 77, 103]	40	77	103	103
[24, 95, 109]	24	95	109	109
[13, 120, 127]	13	120	127	127
[23, 120, 133]	23	120	133	7*19
[65, 88, 133]	65	88	133	7*19

表 5:

[69, 91, 139]	69	91	139	139
[56, 115, 151]	56	115	151	151
[25, 143, 157]	25	143	157	157
[75, 112, 163]	75	112	163	163
[15, 161, 169]	15	161	169	13*13
[104, 105, 181]	104	105	181	181
[32, 175, 193]	32	175	193	193
[56, 165, 199]	56	165	199	199
[29, 195, 211]	29	195	211	211
[17, 208, 217]	17	208	217	7*31
[87, 160, 217]	87	160	217	7*31
[85, 168, 223]	85	168	223	223
[119, 145, 229]	119	145	229	229
[31, 224, 241]	31	224	241	241
[72, 203, 247]	72	203	247	13*19
[93, 187, 247]	93	187	247	13*19
[64, 221, 259]	64	221	259	7*37
[144, 155, 259]	144	155	259	7*37
[19, 261, 271]	19	261	271	271
[95, 217, 277]	95	217	277	277
[133, 192, 283]	133	192	283	283
[40, 279, 301]	40	279	301	7*43
[136, 209, 301]	136	209	301	7*43
[35, 288, 307]	35	288	307	307
[105, 247, 313]	105	247	313	313
[21, 320, 331]	21	320	331	331
[105, 272, 337]	105	272	337	337
[37, 323, 343]	37	323	343	7* 7*7
[111, 280, 349]	111	280	349	349
[185, 231, 361]	185	231	361	19*19
[88, 315, 367]	88	315	367	367
[152, 273, 373]	152	273	373	373
[176, 259, 379]	176	259	379	379
[23, 385, 397]	23	385	397	397
[80, 357, 403]	80	357	403	13*31
[115, 333, 403]	115	333	403	13*31
[161, 304, 409]	161	304	409	409
[41, 399, 421]	41	399	421	421
[123, 352, 427]	123	352	427	7*61
[240, 253, 427]	240	253	427	7*61

表 6:

[48, 407, 433]	48	407	433	433
[205, 299, 439]	205	299	439	439
[240, 287, 457]	240	287	457	457
[43, 440, 463]	43	440	463	463
[25, 456, 469]	25	456	469	7*67
[129, 391, 469]	129	391	469	7*67
[175, 369, 481]	175	369	481	13*37
[215, 336, 481]	215	336	481	13*37
[88, 437, 487]	88	437	487	487
[275, 301, 499]	275	301	499	499
[104, 451, 511]	104	451	511	7*73
[264, 325, 511]	264	325	511	7*73
[208, 387, 523]	208	387	523	523
[184, 425, 541]	184	425	541	541
[135, 473, 553]	135	473	553	7*79
[141, 475, 559]	141	475	559	13*43
[189, 440, 559]	189	440	559	13*43
[235, 416, 571]	235	416	571	571
[297, 368, 577]	297	368	577	577
[329, 351, 589]	329	351	589	19*31
[280, 423, 613]	280	423	613	613
[245, 459, 619]	245	459	619	619
[319, 441, 661]	319	441	661	661
[377, 400, 673]	377	400	673	673
[312, 493, 703]	312	493	703	19*37
[371, 480, 739]	371	480	739	739
[403, 477, 763]	403	477	763	7*109
[448, 495, 817]	448	495	817	19*43

4　考察

この結果から，c を素因数分解すると, 出てくる素数は、前の c に出てきた数になることも同時に分かった.

4.1　方針

では, その c についてもう少し考えてみる. 次は、$a^2+ab+b^2=c$ を満たす, (a,b,c) を考える.

4.1.1　プログラムの実行

```
caabb(C):-
C1 is floor(sqrt(C/3)),
for(1=<C1,A),
B is (-A+sqrt(-3*A*A+4*C))/2,
B1 is floor(B+0.1),
abs(B-B1)<0.0000001,
gcd(D=(A,B1)),D==1,
write(C),put(9),write(A),put(9),write(B1),nl,
fail.
caabb(C).
```

表 7:

c	a	b
3	1	1
7	1	2
13	1	3
19	2	3
21	1	4
31	1	5
37	3	4
39	2	5
43	1	6
49	3	5
57	1	7
61	4	5
67	2	7
73	1	8
79	3	7
91	1	9
91	5	6
93	4	7
97	3	8
103	2	9
109	5	7
111	1	10
127	6	7
129	5	8
133	1	11
133	4	9
139	3	10
147	2	11
151	5	9
157	1	12
163	3	11
169	7	8
181	4	11
183	1	13
193	7	9
199	2	13

表 8:

201	5	11
211	1	14
217	3	13
217	8	9
219	7	10
223	6	11
229	5	12
237	4	13
241	1	15
247	3	14
247	7	11
259	2	15
259	5	13
271	9	10
273	1	16
273	8	11
277	7	12
283	6	13
291	5	14
301	4	15
301	9	11
307	1	17
309	7	13
313	3	16
327	2	17
331	10	11
337	8	13
343	1	18
349	3	17
361	5	16
367	9	13
373	4	17
379	7	15
381	1	19
397	11	12
399	5	17
399	10	13

表 9:

403	2	19
403	9	14
409	8	15
417	7	16
421	1	20
427	3	19
427	6	17
433	11	13
439	5	18
453	4	19
457	7	17
463	1	21
469	3	20
469	12	13
471	11	14
481	5	19
481	9	16
487	2	21
489	8	17
499	7	18

5　考察

この結果より，c に出てくる数は，素数の場合が多く，素数でなくても素因数分解された数は，前に出てきた数となる．（4 の考え方と同様）

5.1　方針

では，次に c を素数と限定して，考えていく．この時，
$c = 3$, または，　$c = 6s + 1$
の形になることを証明する．

5.1.1　証明

① $c = 3$ のとき，$a = 1, b = 1$ より成り立つ．

② a と b を mod6 で考えると，
$a \equiv 1, 3, 5 \bmod 6, b \equiv 1, 3, 5 \bmod 6$
の組を考えることが出来る．この 9 通りの組合せの中で，題意を満たすものを考えていく．

$a \equiv 1 \bmod 6, b \equiv 1 \bmod 6$ の場合，
$a = 6s + 1, b = 6t + 1$ より，
$c = (6s + 1)^2 + (6s + 1)(6t + 1) + (6t + 1)^2$
$= 6(6s^2 + 3s + 3t + 6t^2) + 3$
$= 6s + 3$ よって，この場合は不適．

以下同様にして，証明していくと，

$a \equiv 1 \bmod 6, b \equiv 3 \bmod 6$ の場合，
$c = 6s + 13$
$= 6(s + 2) + 1 \equiv 1 \bmod 6$ よって題意を満たす．

$a \equiv 1 \bmod 6, b \equiv 5 \bmod 6$ の場合，
$c = 6s + 31$
$= 6(s + 5) + 1 \equiv 1 \bmod 6$ よって題意を満たす．

$a \equiv 3 \bmod 6, b \equiv 1 \bmod 6$ の場合，
$c = 6s + 13$
$= 6(s + 2) + 1 \equiv 1 \bmod 6$ よって題意を満たす．

$a \equiv 3 \bmod 6, b \equiv 3 \bmod 6$ の場合，
$c = 6s + 27$
$= 6(s + 4) + 3$ よってこの場合は不適．

$a \equiv 3 \bmod 6, b \equiv 5 \bmod 6$ の場合，
$c = 6s + 49$
$= 6(s + 8) + 1 \equiv 1 \bmod 6$ よって題意を満たす．

$a \equiv 5 \bmod 6, b \equiv 1 \bmod 6$ の場合，

$c = 6s + 31$
$= 6(s + 5) + 1 \equiv 1 \bmod 6$ よって題意を満たす.

$a \equiv 5 \bmod 6, b \equiv 3 \bmod 6$ の場合,
$c = 6s + 49$
$= 6(s + 8) + 1 \equiv 1 \bmod 6$ よって題意を満たす.

$a \equiv 5 \bmod 6, b \equiv 5 \bmod 6$ の場合,
$c = 6s + 75$
$= 6(s + 12) + 3$ よってこの場合は不適.

よって, $c = 6s + 1 (c \equiv 1 \bmod 6)$ の形で表すことが出来た.

6 考察

次に, c が合成数の場合で考える.

$c = 91$ を例にして考えてみよう.

$91 = 7 * 13$ より,
$\overline{\omega} = \frac{-1-\sqrt{3}i}{2}$
$\omega^2 = -\omega - 1 = \frac{1-\sqrt{3}i}{2} - 1 = \frac{-1-\sqrt{3}i}{2}$ より,
$(a - b\omega)(\overline{a - b\omega}) = (a - b\omega)(a - b\omega^2) = a^2 - (\omega^2 + \omega)ab + b^2 = a^2 + ab + b^2$ で表すことが出来る.
よって, ω を使うと, $7 = 1^2 + 1 * 2 + 2^2 = (1 - 2\omega)(1 - 2\omega^2)$
$13 = 1^2 + 1 * 3 + 3^2 = (1 - 3\omega)(1 - 3\omega^2)$ と出来る.
$91 = 13 * 7 = (1 - 2\omega)(1 - 2\omega^2)(1 - 3\omega)(1 - 3\omega^2) * 1$ と考えると,
$(1 = \omega * \omega^2$ より$)$
ここで, $\alpha = (1 - 2\omega)\omega, \beta = (1 - 3\omega)\omega$ とおくと,
$\alpha\beta = (\omega - 2\omega^2)(\omega - 3\omega^2) = \omega^2 + 6\omega - 5$
$= (-\omega - 1) + 6\omega - 5 = -6 + 5\omega$
ゆえに, $a = -6, -b = 5$ とすると,
$91 = 5^2 + 5 * 6 + 6^2$ となることが分かる.

また, $c = 91$ になる a, b は, 表 9 より, $a = 1, b = 9$ ともなるので, それを調べると,
$1 - 9\omega = (1 - 2\omega) * X$ とすると,
$X = \frac{(1-9\omega)(1-2\omega^2)}{(1-2\omega)(1-2\omega^2)}$
$= 3 - \omega$
よって, $-(1 - 3\omega^2) * \omega = 3 - \omega$ より,
$(1 - 3\omega^2)$ に $-\omega$ をかければよいということになる.
ゆえに, $(1 - 2\omega) * -(1 - 3\omega^2) * \omega = 1 - 9\omega$ より,
$a = 1, -b = -9$ と考えると成り立つ.

7　全体の考察

これらの研究から，アイゼンシュタイン数について，c に関して素因数分解すると，非常に特徴が表れることがよくわかる．特に，c が合成数の場合，その数は，前に出てきた素数であり，なおかつ $c = 91$ の場合，ω を使った素因数分解の因数の組合せの仕方によって，a, b が 2 通り出てきた．